Public Key Service

Profil der qualifizierten Signaturzertifikate

Version: 2.2
Stand: 03.09.2019
Status: Freigegeben

Öffentliches Dokument

Business flexibility T · · Systems · · ·

Impressum

Herausgeber
T-Systems International GmbH

Dateiname	Dokumentennummer	Dokumentenbezeichnung
PKS Zertifikatsprofil ECC und RSA2048 qual Sign v2.2.doc		Spezifikation

Version	Stand	Status
2.2	03.09.2019	Freigegeben

Inhaltsverzeichnis

1 Einleitung

Die qualifizierten Zertifikate des Public Key Service gemäß eIDAS Verordnung[1] sind konform zur COMMON-PKI Spezifikation [COMMON-PKI]. Damit ist eine Interoperabilität zu anderen Zertifizierungsstellen gegeben, die diesen Standard unterstützen, und die Zertifikate können von Standard-Clients verarbeitet werden.

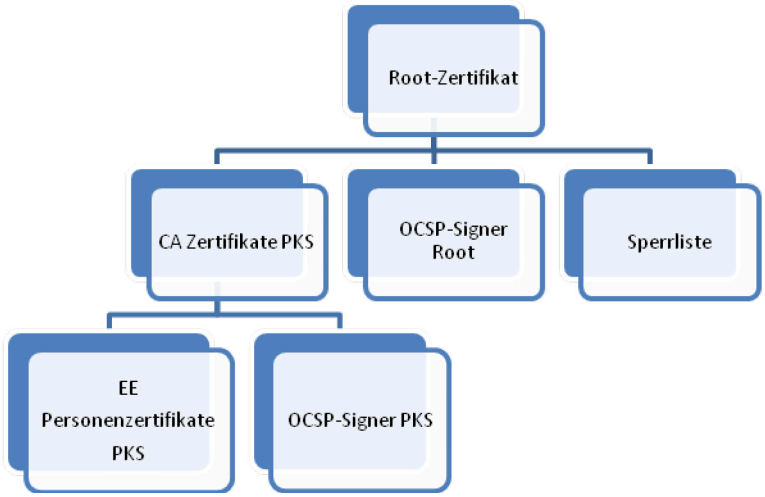
Die COMMON-PKI-Spezifikation [COMMON-PKI] ist eine Profilierung der internationalen PKIX-Standards ist.

Dieses Dokument beschreibt den Aufbau der Zertifikatsinfrastruktur und der qualifizierten Signaturzertifikate. Die in dem jeweiligen Zertifikattyp enthaltenen Daten werden ausgehend von der jeweils grundlegenden Struktur gemäß X.509 [X509] erläutert. Dabei werden die Felder und mögliche Inhalte, sowie die zu verwendenden Datentypen festgelegt.

[1] EU Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

2 Zertifikats Infrastruktur

Die Zertifikats Infrastruktur besteht aus einem Wurzel-Zertifikat, ggf. mehreren Zwischenzertifikaten und den Endbenutzer Zertifikaten so wie Sperrliste und OCSP Responder. Das Nachfolgende Schaubild zeigt die für den Public Key Service verwendete Infrastruktur.



3 Zertifikats- und Sperrlistenprofile der Zertifikatsinfrastruktur

3.1 Wurzel-Zertifikat

Das Root Zertifikat, oder Wurzel-Zertifikat, ist das oberste Zertifikat in der Zertifikats Infrastruktur. Auf dieses Zertifikat lassen sich alle anderen Zertifikate zurückführen.

Feld	Wert	
Version	3	
Seriennummer	11 79 a2 c4 70 e1 21 c3	
Signaturalgorithmus	ecdsa-with-SHA512 (1.2.840.10045.4.3.4)	
Aussteller	CN = TeleSec qualified Root CA 1 organizationIdentifier OID (2.5.4.97) = USt-IdNr. DE 123475223 O = Deutsche Telekom AG C = DE	
Gültigkeitszeitraum	notBefore	5. April 2017 09:30:31
	notAfter	5. April 2047 23:59:59
Inhaber	CN = TeleSec qualified Root CA 1 organizationIdentifier OID (2.5.4.97) = USt-IdNr. DE 123475223 O = Deutsche Telekom AG C = DE	
Öffentlicher Schlüssel	AlgorithmIdentifier	ecPublicKey (1.2.840.10045.2.1)
	Parameter	Secp521r1 (1.3.132.0.35)
	Wert	04 00 15 aa 45 8a 35 b7 55 9f 01 09 76 a9 8a 13 f5 7c 15 22 56 15 ff e9 13 bd b0 a3 35 a6 7c e1 b3 fd 70 e0 eb e8 73 fa 50 92 6e 60 cb c8 6a 1f ab f3 5a 7a 83 59 b5 29 90 4c a0 67 11 5b ef a2 7a 44 16 00 9d 10 35 95 d9 09 87 1b c6 c1 68 94 fc a2 fd 64 0a c6 a9 7f d5 0a 0a 53 6e 2c 22 0d 00 3e 28 cf 45 42 9e 12 a4 c0 1a 94 e6 78 70 bc f5 6c 00 52 62 71 f3 73 92 90 c4 e4 ae cd cb 86 a5 6a ea c3 e3
Zertifikatserweiterungen	SubjectKeyIdentifier	25 8d 2c 22 b8 92 1a 99 f9 34 cb f9 d4 35 ea af c6 b0 1d 0f
	KeyUsage	kritisch crlSign + keyCertSign
	BasicConstraints	Kritisch Ist eine Zertifizierungsstelle Maximale Anzahl an Zwischen-Zertifizierungsstellen: uneingeschränkt
	AuthorityKeyIdentifier	25 8d 2c 22 b8 92 1a 99 f9 34 cb f9 d4 35 ea af c6 b0 1d 0f
Signatur	AlgorithmIdentifier	ecdsa-with-SHA512 (1.2.840.10045.4.3.4)
	Signature	<Bitstring der Signatur>

Fingerprint (SHA256)	2f 82 33 68 9c 6e 9a 75 e2 db 3b 5c 0d 04 ab 12 4d c6 54 9f e9 ce 4c d4 8a 7c a9 ca dc 84 a5 f7

3.2 CA Zertifikat

Das CA Zertifikat, oder Zwischenzertifikat, stellt die Benutzerzertifikate aus. Dieses Zertifikat ist in der Trusted List der EU als vertrauenswürdiges Zertifikat eingetragen.

Feld	Wert	
Version	3	
Seriennummer	00 db cd 76 bd 50 f9 70 f5	
Signaturalgorithmus	ecdsa-with-SHA512 (1.2.840.10045.4.3.4)	
Aussteller	CN = TeleSec qualified Root CA 1 organizationIdentifier OID (2.5.4.97) = USt-IdNr. DE 123475223 O = Deutsche Telekom AG C = DE	
Gültigkeitszeitraum	notBefore	3. Mai 2017 10:45:04
	notAfter	3. Mai 2032 23:59:59
Inhaber	CN = TeleSec PKS eIDAS QES CA 1 organizationIdentifier OID (2.5.4.97) = Ust-IdNr. DE 123475223 O = Deutsche Telekom AG C = DE	
Öffentlicher Schlüssel	AlgorithmIdentifier	ecPublicKey (1.2.840.10045.2.1)
	Parameter	brainpoolP256r1 (1.3.36.3.3.2.8.1.1.7)
	Wert	04 2f 1d e5 89 69 6c 25 b7 fb 1d 05 23 b3 7f 9f 3c 66 f3 9b 69 e2 9b 35 26 80 02 3c b6 02 12 b7 3b 4a 72 09 8e c8 97 00 7d 46 9f 05 ac 31 0d 21 e8 49 4d e6 f4 be e5 ef 6b 41 3c 1b 83 4a dd f6 5e
Zertifikatserweiterungen	SubjectKeyIdentifier	ff f4 89 ea 75 ac c5 d3 d2 24 34 f9 65 2a 06 f2 cc e9 ba 81
	AuthorityKeyIdentifier	25 8d 2c 22 b8 92 1a 99 f9 34 cb f9 d4 35 ea af c6 b0 1d 0f
	KeyUsage	kritisch crlSign + keyCertSign
	BasicConstraints	Kritisch Ist eine Zertifizierungsstelle Maximale Anzahl an Zwischen-Zertifizierungsstellen: uneingeschränkt
	Policy	OID = 1.3.6.1.4.1.7879.13.27 CPS URI: http://pks.telesec.de/cps
	CRLDistributionPoint	http://tqrca1.pki.telesec.de/rl/TeleSec_qualified_Root_CA_1.crl
	AuthorityInfoAccess	(1) OCSP: URI: http://tqrca1.ocsp.telesec.de/ocspr (2) CA-Aussteller: URI: http://tqrca1.pki.telesec.de/crt/ TeleSec_qualified_Root_CA_1.crt
Signatur	AlgorithmIdentifier	ecdsa-with-SHA512 (1.2.840.10045.4.3.4)
	Signature	<Bitstring der Signatur>
Fingerprint (SHA256)	cc 9d 4d cc ce a8 c6 91 aa 72 83 92 c2 d7 df b3	

	1f a3 13 76 7c 84 4b f5 d3 27 76 e7 f8 54 64 d7

3.3 Root OCSP Signer Zertifikat

Dieses OCSP Signaturzertifikat signiert Statusanfragen zu Zertifikaten welche vom Wurzel-Zertifikat ausgestellt wurden. Dieses Zertifikat wird regelmäßig getauscht und ist deswegen hier ohne konkreten Zertifikatsinhalt in den Feldern Seriennummer, Gültigkeitszeitraum und öffentlicher Schlüssel angegeben.

Feld	Wert	
Version	3	
Seriennummer	< 8 Byte langer Zufallswert >	
Signaturalgorithmus	ecdsa-with-SHA256 (1.2.840.10045.4.3.2)	
Aussteller	CN = TeleSec qualified Root CA 1 organizationIdentifier OID (2.5.4.97) = USt-IdNr. DE 123475223 O = Deutsche Telekom AG C = DE	
Gültigkeitszeitraum	notBefore	< Produktionszeitpunkt >
	notAfter	< notBefore + 2 Jahre>
Inhaber	CN = TeleSec eIDAS QES OCSP 1 organizationIdentifier OID (2.5.4.97) = USt-IdNr. DE 123475223 O = Deutsche Telekom AG C = DE	
Öffentlicher Schlüssel	AlgorithmIdentifier	rsaEncryption (1.2.840.113549.1.1.1)
	Parameter	NULL
	Wert	<Schlüsseldaten>
Zertifikatserweiterungen	SubjectKeyIdentifier	SHA1 Hashwert des öffentlichen Schlüssels
	AuthorityKeyIdentifier	25 8d 2c 22 b8 92 1a 99 f9 34 cb f9 d4 35 ea af c6 b0 1d 0f
	KeyUsage	kritisch contentCommitment
	ExtendedKeyUsage	ocspSigning
	OCSPNoCheck	NULL
	AuthorityInfoAccess	CA-Aussteller: URI: http://tqrca1.pki.telesec.de/crt/TeleSec_qualified_Root_CA_1.crt
	BasicConstraints	Kritisch Ist keine Zertifizierungsstelle
	Policy	OID = 1.3.6.1.4.1.7879.13.27 CPS URI: http://pks.telesec.de/cps
	CRLDistributionPoint	http://tqrca1.pki.telesec.de/rl/TeleSec_qualified_Root_CA_1.crl
Signatur	AlgorithmIdentifier	ecdsa-with-SHA256 (1.2.840.10045.4.3.2)
	Signature	<Bitstring der Signatur>

3.4 Sperrliste

Die Sperrliste enthält Sperrinformationen zu Zertifikaten, welche vom Wurzel-Zertifikat ausgestellt wurden. Die Sperrliste enthält die folgenden Inhalte:

Feld	Wert	
Version	2	
Signaturalgorithmus	ecdsa-with-SHA256 (1.2.840.10045.4.3.2)	
Aussteller	CN = TeleSec qualified Root CA 1 organizationIdentifier OID (2.5.4.97) = USt-IdNr. DE 123475223 O = Deutsche Telekom AG C = DE	
Ausstelldatum	<Generierungsdatum der Sperrliste>	
Nächstes Update	<Ausstelldatum plus 6 Monate>	
Gesperrte Zertifikate	Dieses Feld enthält die Liste der gesperrten Zertifikate. Wenn keine gesperrten Zertifikate vorhanden sind, ist das Feld nicht vorhanden.	
Erweiterungen	Laufende Nummer	<laufende Nummer der Sperrliste>
	authorityKeyIdentifier	25 8d 2c 22 b8 92 1a 99 f9 34 cb f9 d4 35 ea af c6 b0 1d 0f
Signatur	<BitString der Signatur>	

Die Sperrliste ist abrufbar von der URL http://tqrca1.pki.telesec.de/rl/TeleSec_qualified_Root_CA_1.crl

3.5 EE OCSP Signaturzertifikate

Diese Zertifikate signieren Statusanfragen zu Benutzerzertifikaten. Zur Lastverteilung sind immer mehrere OCSP-Signaturzertifikate in Betrieb. Diese Zertifikate werden regelmäßig ausgetauscht.

Feld	Wert	
Version	3	
Seriennummer	<4 Byte langer Zufallswert>	
Signaturalgorithmus	ecdsa-with-SHA256 (1.2.840.10045.4.3.2)	
Aussteller	CN = TeleSec PKS eIDAS QES CA 1 organizationIdentifier OID (2.5.4.97) = USt-IdNr. DE 123475223 O = Deutsche Telekom AG C = DE	
Gültigkeitszeitraum	notBefore	< Produktionszeitpunkt >
	notAfter	< notBefore + 2 Jahre>
Inhaber	CN = TeleSec PKS eIDAS QES OCSP <fortlaufende Nummer> organizationIdentifier OID (2.5.4.97) = USt-IdNr. DE 123475223	

	O = Deutsche Telekom AG C = DE	
Öffentlicher Schlüssel	AlgorithmIdentifier	ecPublicKey (1.2.840.10045.2.1)
	Parameter	brainpoolP256r1 (1.3.36.3.3.2.8.1.1.7)
	Wert	<Schlüsseldaten>
Zertifikatserweiterungen	SubjectKeyIdentifier	SHA1 Hashwert des öffentlichen Schlüssels
	AuthorityKeyIdentifier	`ff f4 89 ea 75 ac c5 d3 d2 24 34 f9 65 2a 06 f2 cc e9 ba 81`
	KeyUsage	kritisch contentCommitment
	ExtendedKeyUsage	ocspSigning
	AuthorityInfoAccess	(1) OCSP: URI: http://pks.telesec.de/ocspr (2) CA-Aussteller: URI: http://tqrca1.pki.telesec.de/crt/crt/TeleSec_PKS_eIDAS_QES_CA_1.crt
	BasicConstraints	Kritisch Ist keine Zertifizierungsstelle
	Policy	OID = 1.3.6.1.4.1.7879.13.27 CPS URI: http://pks.telesec.de/cps
Signatur	AlgorithmIdentifier	ecdsa-with-SHA256 (1.2.840.10045.4.3.2)
	Signature	<Bitstring der Signatur>

4 Profil der Benutzerzertifikate

Die folgende Tabelle zeigt alle möglichen Felder innerhalb des Zertifikates, die von TeleSec genutzt werden. Felder und Zertifikatserweiterungen (Extensions), die personalisierten Inhalt enthalten, werden in den nachfolgenden Kapiteln erläutert.

Feld	Wert	
Version	3	
Seriennummer	<4 Byte langer Zufallswert>	
Signaturalgorithmus	ecdsa-with-SHA256 (1.2.840.10045.4.3.2)	
Aussteller	CN = TeleSec PKS eIDAS QES CA 1 organizationIdentifier OID (2.5.4.97) = USt-IdNr. DE 123475223 O = Deutsche Telekom AG C = DE	
Gültigkeitszeitraum	notBefore	< Produktionszeitpunkt >
	notAfter	< je nach Beauftragung >
Inhaber	Pflichtfelder: CN: C: SerialNumber: Optional: SN: GN: O: OU: Pseudonym:	
Öffentlicher Schlüssel	AlgorithmIdentifier	ecPublicKey (1.2.840.10045.2.1)
	Parameter	brainpoolP256r1 (1.3.36.3.3.2.8.1.1.7)
	Wert	<Schlüsseldaten>
Zertifikatserweiterungen	SubjectKeyIdentifier	SHA1 Hashwert des öffentlichen Schlüssels
	AuthorityKeyIdentifier	`ff f4 89 ea 75 ac c5 d3 d2 24 34 f9 65 2a 06 f2 cc e9 ba 81`
	KeyUsage	kritisch contentCommitment
	BasicConstraints	Kritisch Ist keine Zertifizierungsstelle
	Policy	QCP-n-qscd (0.4.0.194112.1.2) CPS URI: http://pks.telesec.de/cps
	QCStatement	esi4-qcStatement-1 id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) esi4-qcStatement-4 id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) esi4-qcStatement-5 (0.4.0.1862.1.5)

		QC-STATEMENT ::= { SYNTAX QcEuPDS IDENTIFIED BY id-etsi-qcs-QcPDS } QcEuPDS ::= PdsLocations PdsLocations ::= SEQUENCE SIZE (1..MAX) OF PdsLocation PdsLocation::= SEQUENCE { url IA5String = "http://www.telesec.de/signaturkarte/agb", language PrintableString (SIZE(2) = "DE")}
	AuthorityInfoAccess	(1) OCSP: URI: http://pks.telesec.de/ocspr (2) CA-Aussteller: URI: http://tqrca1.pki.telesec.de/crt/TeleSec_PKS_eIDAS_QES_CA_1.crt
	Ggf. weitere optionale Extensions	SubjectAltName, Restriction, Admission, Procuration, usw.
Signatur	AlgorithmIdentifier	ecdsa-with-SHA256 (1.2.840.10045.4.3.2)
	Signature	<Bitstring der Signatur>

4.1 Das Feld SerialNumber

In diesem Feld wird die Zertifikatsnummer abgelegt.

4.2 Das Feld Signaturalgorithmus

Das Feld `Signature` enthält den Bezeichner des Signaturalgorithmus, der von der CA für die Erstellung des Zertifikates benutzt wird.

Abhängig von der Generation der Benutzerzertifikate werden unterschiedliche Algorithmen benutzt.

- Ecdsa-with-SHA256 {1.2.840.10045.4.3.2} ab 01.08.2017
- RSA-PSS {1.2.840.113549.1.1.10} ab 10.12.2015
- sha-256WithRsaEncryption {1.2.840.113549.1.1.11} ab 31.12.2007
- vor 31.12.2007 sha1WithRSAEncryption

4.3 Das Feld Aussteller

In dem Feld `Issuer` wird der Name des Herausgebers abgelegt. Der Inhalt dieses Feldes muss exakt mit dem Inhalt des Subject-Feldes des CA-Zertifikates übereinstimmen, von dem das Benutzerzertifikat unterschrieben worden ist.

Folgende Attribute werden verwendet:

- countryName (vorgeschrieben)
- organizationName (vorgeschrieben)
- organizationalUnitName (optional)
- commonName (vorgeschrieben)
- pseudonym (bedingt, muss verwendet werden, wenn sich im commonName ein pseudonym befindet)
- organizationIdentifier (bedingt, muss verwendet werden, wenn sich im commonName dieses Feld befindet. Dieses Feld wird durch die eIDAS Verordnung gefordert wenn das Zertifikat für eine juristische Person ausgestellt wurde. Dies ist bei den eIDAS konformen CA Zertifikaten der Fall)

Anmerkung:

Der Inhalt des Feldes Issuer wird aus dem Subject-Feld des CA-Zertifikates entnommen von dem das Zertifikat unterschrieben werden soll.

4.4 Das Feld Gültigkeitszeitraum

In diesem Feld wird der Gültigkeitszeitraum des Zertifikates eingetragen. Der Inhalt des Feldes hat folgende Syntax:

```
Validity ::= SEQUENCE
{
    notBefore     Time
    notAfter      Time
}

Time ::= CHOICE
{
    utcTime    UTCTime
    generalizedTime GeneralizedTime
}
```

Die Uhrzeit wird bis zum Jahr 2049 als UTCTime kodiert werden. Ab dem Jahr 2050 wird die Kodierung GeneralizedTime verwendet.

4.5 Das Feld Inhaber

Der Name des Zertifikatsinhabers wird in dem Feld `Subject` gespeichert. Der Name für den Zertifikatsinhaber muss innerhalb der Zertifizierungsstelle für die komplette Lebensdauer der CA eindeutig sein.

Folgende Attribute werden verwendet:

- countryName (vorgeschrieben)
- organizationName (optional)
- organizationalUnitName (optional)
- commonName (vorgeschrieben)
- serialNumber (vorgeschrieben)
- pseudonym (bedingt vorgeschrieben s.u.)
- surname (bedingt vorgeschrieben s.u.)
- givenname (bedingt vorgeschrieben s.u.)

Wenn der Zertifikatsinhaber ein Pseudonym als Name wünscht, wird zusätzlich das Attribut Pseudonym kodiert. Der Pseudonym-Name befindet sich immer in den Attributen commonName und pseudonym. Hierbei wird ein Pseudonym mit der Endung „:PN“ gekennzeichnet.

Die Attribute surname/givenname und pseudonym schließen sich gegenseitig aus. Wenn im Zertifikat ein Pseudonym eingetragen ist werden surname/givenname nicht verwendet. Wird kein Pseudonym verwendet so sind die Felder surname und givenname erforderlich.

Das Feld hat die gleiche Datenstruktur wie das Feld Issuer (siehe Kapitel 4.3).

4.6 Das Feld Öffentlicher Schlüssel

Der PublicKey des Zertifikatsinhabers wird in diesem Feld zusammen mit dem Algorithmus für den Gebrauch des Schlüssels gespeichert.

Ab dem 01.01.2015 werden nur noch Zertifikate mit Schlüsseln basierend auf elliptischen Kurven ausgegeben. Als Algorithmus wird die OID ecPublicKey {1 2 840 10045 2 1} verwendet. Zertifikate, die vor dem 01.12.2012 ausgestellt wurden enthalten Schlüssel vom Typ rsaEncryption {1 2 840 113549 1 1 1} verwendet..

Der Inhalt des Feldes hat folgende Syntax:

```
SubjectPublicKeyInfo ::= SEQUENCE
{
    algorithm       AlgorithmIdentifier
    subjectPublicKey     BIT STRING
}
AlgorithmIdentifier ::= SEQUENCE
{
    algorithm       OBJECT IDENTIFIER
    parameters      ANY DEFINED BY algorithm OPTIONAL
}
```

Das Feld `parameters` kann zusätzliche Parameter des Algorithmus enthalten. Für den verwendeten Algorithmus (RSA) werden sie jedoch nicht benötigt, deshalb ist dieses Feld Null (explizit NULL). Für Schlüssel basierend auf elliptischen Kurven wird hier die OID der Kurve eingetragen. Für diesen Zertifizierungsbereich wird die Kurve brainpoolP256r1 (OID { 1 3 36 3 3 2 8 1 1 7}) verwendet. Die Codierung erfolgt immer als benannte Kurve.

4.7 Das Feld Signatur

Dieses Feld enthält die Signatur des Zertifikates, die von der Zertifizierungsstelle erzeugt worden ist.

4.8 Das Feld Zertifikatserweiterungen

Die Extensions dienen zur Erweiterung der im Zertifikat enthaltenen Daten. Es gibt mehrere verschiedene Extensions, die in den folgenden Unterkapiteln aufgeführt werden.

Die Extensions haben folgende Syntax:

```
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension
Extension ::= SEQUENCE
{
 extnId     OBJECT IDENTIFIER
 critical      BOOLEAN DEFAULT FALSE
 extnValue     OCTET STRING
}
```

Der Wert `extnId` gibt mit Hilfe eines Object Identifiers den Typ der in `extnValue` enthaltenen Extension an. Das Flag `critical` zeigt an, ob die Extension als kritisch markiert worden ist. Wenn `critical` auf TRUE gesetzt wird, bedeutet dies, dass der Client das Zertifikat als ungültig betrachten muss, wenn er die Extension nicht auswerten kann.

4.8.1 Die Extension SubjectAltNames (optional)

Mit Hilfe dieser Extension können alternative Namen für den Zertifikatsinhaber im Zertifikat eingefügt werden.

Diese Extension wird als nicht kritisch markiert.

Die Extension hat folgende Datenstruktur:

```
SubjectAltNames ::= GeneralNames
```

Wenn diese Extension vorhanden ist enthält sie genau eine E-Mail-Adresse des Zertifikatsinhabers als `rfc822Name`.

4.8.2 Die Extension LiabilityLimitationFlag (bedingt vorgeschrieben)

Mit dieser Extension wird angezeigt, dass ein Attributzertifikat existiert, durch das die Verwendung dieses Zertifikats eingeschränkt wird.

Die Extension wird als nicht kritisch markiert.

Die Extension hat den folgenden Aufbau:

```
LiabilityLimitationFlag ::= BOOLEAN
```

Der Wert des Flags wird immer auf TRUE gesetzt. Wenn keine Einschränkung vorhanden ist, wird die Extension nicht benutzt. Seit Umsetzung der eIDAS Verordnung werden keine Attributzertifikate mehr produziert. Somit wird diese Extension nicht mehr benötigt. Ihre Beschreibung an dieser Stelle bleibt erhalten wegen der ehemaligen Nutzung der Extension.

4.8.3 Die Extension Procuration (optional)

Diese Extension wird verwendet, wenn der Zertifikatsinhaber für eine andere Person Unterschriften leisten darf.

Diese Extension wird als nicht kritisch markiert.

Die Extension hat den folgenden Aufbau:

```
ProcurationSyntax ::= SEQUENCE
{
 country      [1] EXPLICIT PrintableString OPTIONAL
 typeOfSubstitution[2] EXPLICIT DirectoryString OPTIONAL
 signingFor      [3] EXPLICIT SigningFor
}

SigningFor ::= CHOICE
{
 thirdPerson  GeneralName
 certRef    IssuerSerial
}

IssuerSerial ::= SEQUENCE
{
 issuer     GeneralNames
 serial     CertificateSerialNumber
 issuerUID    UniqueIdentifier OPTIONAL
}
```

Es wird das Feld `thirdPerson` in der Sequence `SigningFor` verwendet dieses kann alle Attribute aus Anhang A enthalten.

Die Länge des Feldes `typeOfSubstitution` wird auf eine Länge von 128 Bytes begrenzt. Der Datentyp für dieses Feld ist PrintableString.

4.8.4 Die Extension Admission (optional)

Diese Extension Admission wird verwendet, um Informationen über die Berechtigung bestimmte Aufgaben erledigen zu dürfen in das Zertifikat aufzunehmen.

Diese Extension wird als nicht kritisch markiert.

Die Extension Admission hat die folgende Datenstruktur:

```
AdmissionSyntax ::= SEQUENCE
{
 admissionAuthority   GeneralName OPTIONAL
 contentsOfAdmissions    SEQUENCE OF Admissions
}
Admissions ::= SEQUENCE
{
 admissionAuthority[0] EXPLICIT GeneralName OPTIONAL
 namingAuthority    [1] EXPLICIT] NamingAuthority OPTIONAL
 professionInfos    SEQUENCE OF ProfessionInfos
}

NamingAuthority ::= SEQUENCE
{
 namingAuthorityId    OBJECT IDENTIFIER OPTIONAL
 namingAuthorityUrl   IA5String OPTIONAL
 namingAuthorityText     DirectoryString OPTIONAL
}

ProfessionInfo ::= SEQUENCE
{
 namingAuthority    [0] EXPLICIT NamingAuthority OPTIONAL
 professionItems    SEQUENCE OF DirectoryString
 professionOIDs     SEQUENCE OF OBJECT IDENTIFIER Optional
 registrationNumberPrintableString OPTIONAL
 addProfessionInfo OCTET STRING OPTIONAL
}
```

Das Feld `admissionAuthorithy` wird immer nur an einer Stelle kodiert. Wenn alle vorhandenen Bestätigungen von einer Instanz bestätigt wurden, wird das Feld in der Sequence `AdmissionSyntax` genutzt. Andernfalls muss das Feld in der Sequence `Admissions` verwendet werden. Der Inhalt des Feldes ist ein DirectoryName, der sich aus den Attributen aus Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** und den zusätzlichen Attributen OrganizationName und OrganizationalUnitName zusammensetzt.

In dem Feld `namingAuthorithy` befinden sich Informationen über den Aussteller der Bestätigungen. Wenn alle Bestätigungen von einer Instanz ausgestellt worden sind, wird das entsprechende Feld in der Sequence `Admissions` genutzt. Andernfalls muss das Feld in der Sequence `ProfessionInfos` benutzt werden. Wenn in dem Feld `namingAuthorityText` Informationen vorhanden sind, müssen diese als UTF8-String kodiert werden.

Für den Inhalt des Feldes `professionItems` wird die Kodierung PrintableString benutzt.

4.8.5 Die Extension Restriction (optional)

Diese Extension kann für die Aufnahme von Einschränkungen in das Zertifikat aufgenommen werden.

Diese Extension wird als nicht kritisch markiert.

Die Extension Restriction hat die folgende Datenstruktur:

```
RestrictionSyntax ::= DirectoryString
```

Die Länge des Strings ist grundsätzlich auf 1024 Zeichen beschränkt, bedingt durch den verfügbaren Speicherplatz auf der Chipkarte kann die verfügbare Länge aber noch weiter eingeschränkt werden. Der Inhalt der Extension `Restriction` wird als PrintableString kodiert.

4.8.6 Die Extension AdditionalInformation (optional)

Diese Extension wird für die Integration von Informationen mit nicht einschränkendem Charakter in das Zertifikat verwendet.

Die Extension AdditionalInformation hat die folgende Datenstruktur:

```
AdditionalInformationSyntax ::= DirectoryString
```

Die Länge des Strings wird auf 2000 Zeichen beschränkt. Der Inhalt der Extension `AdditionalInformation` wird als PrintableString kodiert.

Anhang A: Verwendete Attributtypen

Name des Attributs	Object Identifier	ASN.1 String Typ	maximale Länge
commonName	{id-at 3}	UTF8	64
surName	{id-at 4}	UTF8	64
givenName	{id-at 42}	UTF8	64
serialNumber	{id-at 5}	PrintableString	64
organizationIdentifier	{id-at 97}	UTF8	64
title	{id-at 12}	UTF8	64
organizationName	{id-at 10}	UTF8	64
organizationalUnit-Name	{id-at 11}	UTF8	64
BusinessCategory	{id-at 15}	UTF8	128
localityName	{id-at 7}	UTF8	128
stateOrProvinceNa-me	{id-at 8}	UTF8	128
countryName	{id-at 6}	PrintableString	2 (ISO 3166 Code)
distinguished-NameQualifier	{id-at 46}	PrintableString	64
initials	{id-at 43}	UTF8	64
generationQualifier	{id-at 44}	UTF8	64
eMailAddress	{pkcs-9 1}	IA5String	128
domainComponent	{0 9 2342 19200300 100 1 25}	IA5String	definiert in RFC 2247
postalAddress	{id-at 16}	SEQUENCE SIZE (1..6) OF UTF8	6 * 30, Verwendung wird in RFC 3039 beschrieben
pseudonym	{pkix 9 3}	UTF8	64
dateOfBirth	{id-pda 1}	GeneralizedTime	15
placeOfBirth	{id-pda 2}	UTF8	128
gender	{id-pda 3}	PrintableString SIZE (1)	Inhalt: „M“ oder „F“
countryOfCitizenship	{id-pda 4}	PrintableString	2 (ISO 3166 Code)
countryOfResidence	{id-pda 5}	PrintableString	2 (ISO 3166 Code)
nameAtBirth	{id-isismtt-at 14}	UTF8	64

Für die UTF8-Kodierung wird einen Auszug aus dem UTF8-Zeichensatz verwendet, der nur ANSI / ISO 8859-1 Zeichen (Unicode Latin-1 Seite) enthält. Andere Zeichen, die nicht in diesem Zeichensatz enthalten sind, dürfen nicht benutzt werden.

Besonderheiten für bestimmte Attribute:

- commonName: Ein Pseudonym wird immer mit der Endung „:PN“ als Common-Name eingefügt werden. Zusätzlich wird der gleiche Inhalt (einschließlich der Endung) in dem Attribut pseudonym eingefügt.

- postalAddress: Die Adresse wird komplett in diesem Attribut gespeichert. z.B.

    1. Element: Turmstraße 123
    2. Element: 10123 Berlin
    3. Element: Germany.

- DateOfBirth: Das Geburtsdatum wird im GeneralizedTime-Format kodiert. Der Teil mit der Angabe der Uhrzeit wird mit „0“ gefüllt (z.B. 19720508000000Z).

Abkürzungsverzeichnis

CA	Certification Authority
ECC	Elliptic Curve Cryptography ist ein asymmetrisches kryptographisches Verfahren
HTTP	Hypertext Transmission Protocol
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PN	Pseudonym
RSA	RSA (Rivest, Shamir und Adleman) ist ein asymmetrisches kryptographisches Verfahren

Literaturverzeichnis

[COMMON-PKI] Common-PKI COMMON PKI SPECIFICATIONS FOR INTEROPERABLE APPLICATIONS VERSION 2.0 – 20 JANUARY 2009

[X509] Recommendation X.509: The Directory – Authentication Frame